Faculty of Science, Technology, Engineering and Mathematics
M303 Further pure mathematics

M303

TMA 05 2020J

Mainly covers Book E *Rings and fields*
Cut-off date 30 March 2021

You will find instructions for completing TMAs in the 'Assessment' area of the M303 website. Please remind yourself of these instructions before beginning work on this TMA. You can submit this TMA either by post, together with a completed TMA form (PT3), to arrive by the cut-off date given above, or electronically, as a single PDF file, using the University's online TMA/EMA service.

Half of the TMA is formative, and the other half is summative. The formative questions are designed to either *extend* your understanding of the topics or *introduce* the topics of later books, while the summative questions place more emphasis on *assessing* your understanding of the topics. Both types of question will be marked by your tutor, but (unlike the summative questions) marks for the formative questions do not count towards your final grade. You should submit your solutions to both sets of questions to your tutor by the cut-off date.

The marks allocated to each part of a question are indicated in the margin.

Although many of the questions on this assignment require numerical answers, the questions invariably carry *method marks*.

In phrasing the questions, we have used the words listed below, each of which should be interpreted as indicated.

prove, show, explain, justify	Clear reasoning and explanation for all steps are called for.
determine, find, devise, calculate, compute	An indication of the method used and all working in arriving at an answer should be given.
deduce	Clear explanation of how one result follows from another is required.
solve	Working must be shown. A numerical answer alone is not sufficient.
evaluate, give, write down, list	Answer suffices. No explanation need be given.
hence	No marks will be awarded for any alternative method.

Copyright © 2020 The Open University

This TMA is based on Book E (Rings and fields), except for the formative Question 7, which covers the start of Book F.

Part A, consisting of Questions 1–4, 5A, 5B and 6, worth a total of 50 marks, is **summative**. Full marks may be obtained by completing correctly Questions 1–4 and 6, and **one** of 5A, 5B. You should submit only one of 5A and 5B.

The Part A questions assess your knowledge of the module. You must not discuss these questions in the forums, and your tutor is not allowed to help you directly.

Questions 1 and 3 of Part A are designed to enable you to demonstrate understanding of definitions and basic concepts, and to practise calculations that should become routine or are similar to those in Exercises of Book E, while the remaining questions of Part A (except for Question 6) may be a bit more challenging.

Part B is **formative**. You should choose two questions to submit to your tutor for feedback, and we suggest that one of these is Question 7 since this will help you with the next TMA.

Doing the Part B questions will help you to understand key concepts covered in the text. You are encouraged to discuss these questions in the module forums and with your tutor (who is allowed to help you).

Your tutor will mark all of the answers that you submit. But note that only your marks for Part A count towards your overall assessment score.

Part A Summative

Question 1 – 9 marks

In this question you will practise working with ideals in rings that are extensions of degree 2 over the integers. It involves a number of concepts from Chapter 17.

Let R be the ring $\mathbb{Z}[\sqrt{-5}\,]$.

(a) Let A be a subset of R defined by

$$A = \{s + t\sqrt{-5} : s, t \in \mathbb{Z},\ s - t \equiv 0 \,(\mathrm{mod}\ 3)\}.$$

Show that A is an ideal in the ring R. [5]

(b) The subset

$$B = \{u + v\sqrt{-5} : u, v \in \mathbb{Z},\ u + v \equiv 0 \,(\mathrm{mod}\ 3)\}$$

is also an ideal in the ring R (you do not need to prove this). Show that $AB = \langle 3 \rangle$. [4]

Question 2 – 10 marks

This question tests your ability to deal with field extensions. You will need to use concepts and results from Chapters 17 and 18.

Let n be a positive integer that is not a perfect square.

(a) (i) Show that $\sqrt{n} \notin \mathbb{Q}(\sqrt{-n})$ and $\sqrt{-n} \notin \mathbb{Q}(\sqrt{n})$. [3]

(ii) Deduce that the degree $[\mathbb{Q}(\sqrt{n}, \sqrt{-n}) : \mathbb{Q}]$ is equal to 4. [2]

(b) Let $\alpha = \sqrt{n} + \sqrt{-n}$.

(i) By evaluating $\alpha^3 + 2n\alpha$ and $\alpha^3 - 2n\alpha$, show that $\mathbb{Q}(\sqrt{n}, \sqrt{-n}) \subseteq \mathbb{Q}(\sqrt{n} + \sqrt{-n})$. [2]

(ii) Deduce that $\mathbb{Q}(\sqrt{n}, \sqrt{-n}) = \mathbb{Q}(\sqrt{n} + \sqrt{-n})$. [1]

(iii) Determine the *minimal* polynomial for $\alpha = \sqrt{n} + \sqrt{-n}$ over $\mathbb{Q}$. [2]

Hint: begin by evaluating α^2.

Question 3 – 9 marks

In this question you are asked to perform calculations in a finite field. It is based on concepts developed in Chapter 18.

The polynomial $x^4 + x + 1$ is irreducible over the field $\mathbb{Z}_2$ (you do not need to prove this; note that $-1 = +1$ in $\mathbb{Z}_2$), so $\mathbb{Z}_2[x]/(x^4 + x + 1)$ is a field that may be described equivalently in the form $F = \mathbb{Z}_2(\omega)$, where $\omega^4 = \omega + 1$; the order of F is $2^4 = 16$. By Proposition 1.7 of Chapter 18, every element of F can be written in a unique way in the form $a + b\omega + c\omega^2 + d\omega^3$ for some $a, b, c, d \in \mathbb{Z}_2$.

(a) Show that for every element $z \in F$, we have $z + z = 0$. [1]

(b) With the help of one of the methods explained in Worked Exercises 3.10 and 3.11 of Chapter 18, or otherwise, find the multiplicative inverse of the element $1 + \omega^2$ in F. [4]

(c) Show that $\omega^3 \neq 1$ and $\omega^5 \neq 1$. Hence show that ω is a primitive element of F. [4]

Question 4 – 9 marks

This question tests your skills in handling splitting fields and extensions of the field of rational numbers. You will need to use concepts and results from Chapters 17 and 18.

Let F be a field of characteristic distinct from 2, in which the element $2\ (= 1 + 1)$ does not have a square root. Let $E = F(\omega)$ be the smallest field containing F and an element ω such that $\omega^2 = 2$. By Theorem 2.19 of Chapter 18, elements of E have the form $a + b\omega$ for $a, b \in F$.

(a) Show that if $b \neq 0$, then every element $a + b\omega \in E$ is a root of a quadratic polynomial with coefficients in F.

Hint: begin by calculating the square of $a + b\omega$. [4]

(b) Show that $a - b\omega$ is another root of the polynomial found in part (a). [2]

(c) Show that E is a splitting field over F of every quadratic polynomial found in part (a). [2]

(d) Show that the element $3 + 2\omega \in E$ has a square root in E. [1]

Question 5A (constructibility) – 10 marks

This question is designed to test your understanding of (im)possibility of construction with the help of ruler and compasses. It builds on the material of Chapter 19.

Duplication of a cube and quadrature of a circle are two classical problems of Greek geometry. Let us consider their analogues, namely the problems of 'triplicating a cube' and 'cubing a ball'. Triplicating a cube means constructing a cube of three times the volume of a given cube, and cubing a ball means constructing a cube of the same volume as a given ball; in both cases, 'constructing' refers to using ruler and compasses only. We may also assume that the given cube has unit side length and the given ball has unit radius.

(a) Show that a unit cube cannot be triplicated by a construction using ruler and compasses only, following the steps below.

  (i) Show that if a unit cube can be triplicated using ruler and compasses only, then $u = \sqrt[3]{3}$ is a constructible number. [*2*]

  (ii) Find the minimal polynomial for u over $\mathbb{Q}$, and apply Corollary 2.8 of Chapter 19. [*3*]

(b) Show that a unit ball cannot be cubed by a construction using ruler and compasses only, following the steps below.

  (i) Show that if a unit ball can be cubed using ruler and compasses only, then $v = \sqrt[3]{4\pi/3}$ is a constructible number. [*2*]

  (ii) Show that v is transcendental over $\mathbb{Q}$, and apply Theorem 2.7 of Chapter 19. [*3*]

Question 5B (encryption) – 10 marks

This question tests your knowledge of encryption and decryption using the RSA method. The numbers involved are deliberately chosen to be small enough to focus on your understanding without excessive calculations.

Alice and Bob decide to use an RSA cryptosystem with public key $(77, 13)$ for communication.

(a) Alice wants to send Bob the message $m = 29$. Determine Alice's ciphertext c. [*4*]

(b) Determine Bob's private key. [*2*]

(c) Carry out Bob's decryption of Alice's ciphertext c, and compare his result with Alice's message. [*4*]

Question 6 – 3 marks

This question can be done at any point during your study of Book E.

An important part of being a mathematician is being able to communicate mathematics using mathematical notation in different settings. For this TMA, we would like you to post something in the Book E forum that is about the mathematics in M303 and contains mathematical notation. There is a forum post explaining how to use mathematical notation in the Book E forum.

To earn full marks, provide either a screenshot of your forum post or directions as to where to find it (giving thread title, time and date). (If you are not in a position to provide such evidence, or if you cannot use the forum for any reason, contact your tutor for advice.) [*3*]

Part B Formative

Question 7 – 10 marks

This question is designed to help you to practise techniques relevant to Question 1 in TMA 06. It concerns material covered in Chapter 21 of Book F.

Let d be the Euclidean metric on $\mathbb{R}^2$ given by

$$d\big((x_1, y_1), (x_2, y_2)\big) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2},$$

for $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$.

Consider the following four sets in $\mathbb{R}^2$:

$$W = \{(x, y) \in \mathbb{R}^2 : y < \pi\} \cup \{(x, y) \in \mathbb{R}^2 : y > \pi \text{ and } y \leq 7\},$$
$$X = \{(x, y) \in \mathbb{R}^2 : x = y\} \cup \{(x, 3) \in \mathbb{R}^2 : x \in \mathbb{R}\},$$
$$Y = \{(q, \pi) \in \mathbb{R}^2 : q \in \mathbb{Q}\},$$
$$Z = \{(x, y) \in \mathbb{R}^2 : x^2 + (y - \pi)^2 = \pi^2\} \cup \{(x, y) \in \mathbb{R}^2 : x^2 + (y + \pi)^2 < \pi^2\}.$$

For each set, do the following.

(a) On a separate diagram, sketch the set, by hand or otherwise. (If you are unsure how to represent something on a diagram, or are unable to sketch it, then describe what you mean in words. You are also free to use a combination of sketching and writing.) [*4*]

(b) Write down whether the set is d-connected or d-disconnected. If the set is d-disconnected, then write down a d-disconnection. [*6*]

Hint: when using the Euclidean metric, it is always worth guessing.

Question 8 – 10 marks

This question tests your calculation skills in rings of the form $\mathbb{Z}[\sqrt{-n}\,]$. It involves a number of concepts from Chapter 17 and also the concepts of prime and irreducible elements of a ring, introduced and studied earlier in Section 2, and specifically in Subsection 2.2, of Chapter 12.

Let $n \geq 3$ be an odd positive integer that is not a perfect square, and let $R = \mathbb{Z}[\sqrt{-n}\,]$, with multiplicative norm $N(r + s\sqrt{-n}) = r^2 + ns^2$ for every element $r + s\sqrt{-n} \in R$. Let $p \in \mathbb{Z}$, $p \geq 2$, be a prime in $\mathbb{Z}$ such that p divides $n + 1$.

(a) By finding distinct factorisations of $n + 1$ in R, show that p is not a prime in R. [3]

Hint: see the solution to Exercise 2.13(b) of Chapter 17.

(b) Show that there is no element $r + s\sqrt{-n} \in R$, for $r, s \in \mathbb{Z}$, with norm equal to p. [3]

Hint: determine first which of the two numbers p, n is smaller than the other.

(c) With the help of the result of part (b), or otherwise, show that p is an irreducible element of R. [4]

Question 9 – 8 marks

This is a question on the material of Chapter 18, Section 2, about fields and their extensions. It aims to test and develop your skills in handling extensions of the field $\mathbb{Q}$ of rational numbers by adjoining algebraic elements.

(a) Determine the minimal polynomials for $\sqrt[3]{7}$ and $\sqrt[4]{7}$ over $\mathbb{Q}$, and determine the degrees $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}]$ and $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}]$. [3]

(b) By considering common factors of the degrees found in part (a), or otherwise, show that $\sqrt[3]{7} \notin \mathbb{Q}(\sqrt[4]{7})$. [2]

(c) Hence determine the degree $[\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) : \mathbb{Q}]$. [1]

(d) Show that $\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) = \mathbb{Q}(\sqrt[3]{7} \cdot \sqrt[4]{7}) = \mathbb{Q}(\sqrt[12]{7})$. [2]

Hint: express the various roots of 7 as powers of $7^{1/12}$.

Question 10 – 11 marks

This is a question on the material of Chapter 18, Section 2, about fields and their extensions. It aims to test and develop your skills in handling extensions of finite fields by adjoining algebraic elements.

Consider the finite field $F = \mathbb{Z}_5(\omega)$, where $\omega^2 = -3 - 2\omega = 2 + 3\omega$; the order of F is $5^2 = 25$. Proposition 1.7 of Chapter 18 tells us that every element of F can be written uniquely in the form $a + b\omega$ for some $a, b \in \mathbb{Z}_5$.

By Theorem 3.3 of Chapter 18, the multiplicative group of F is cyclic, of order $5^2 - 1 = 24$. In particular, if ξ is a primitive element of F (Definition 3.4 of Chapter 18), then every non-zero element of F is equal to ξ^i for some i such that $0 \leq i \leq 23$.

(a) Determine ω^3 and ω^6 in the form $a + b\omega$ for suitable $a, b \in \mathbb{Z}_5$. [2]

(b) Show that ω is a primitive element of $\mathbb{Z}_5(\omega)$. [3]

(c) By one of the methods explained in Worked Exercises 3.10 and 3.11 of Chapter 18, or otherwise, determine the multiplicative inverse ω^{-1} of ω in the form $\omega^{-1} = a + b\omega$ for suitable $a, b \in \mathbb{Z}_5$. [2]

(d) With the help of Corollary 3.5 of Chapter 18, determine all primitive elements of $\mathbb{Z}_5(\omega)$ in the form $a + b\omega$ for suitable $a, b \in \mathbb{Z}_5$. [4]

Question 11A (constructibility) – 11 marks

This question is designed to test your understanding of (im)possibility of construction with the help of ruler and compasses. It builds on the material of Chapter 19.

(a) Assume that you have a ruler with marks at 0, 1 and $\sqrt[6]{2}$. Determine if it is possible to square a circle of radius $\sqrt{2}$ with such a ruler and compasses. [4]

(b) Assume that you have a ruler with marks at 0, 1 and π^2. Determine if it is possible to square a circle of radius $\sqrt{2}$ with such a ruler and compasses. [3]

(c) Determine if it is possible to duplicate a unit cube with compasses and a ruler with marks at 0, 1 and $\sqrt[3]{4}$. [2]

(d) *Triplicating* a unit cube means constructing a side of a cube of volume 3. Determine if it is possible to triplicate a unit cube with compasses and a ruler with marks at 0, 1 and $\sqrt[6]{3}$. [2]

Question 11B (encryption) – 11 marks

In this question you are asked to demonstrate your knowledge of encryption and decryption in cryptosystems based on elliptic curves over finite fields, covered in Chapter 20. The numbers involved are deliberately chosen to be small enough to focus on your understanding without excessive calculations.

Alice and Bob want to communicate using the Diffie–Hellman–ElGamal system based on the elliptic curve E over GF_{11} given by the equation $y^2 = x^3 + 2x + 5$, with the point $P = (0, 4)$. Bob decided to have $s_B = 2$ as his private key. By experimenting in the group $(E, +)$, Alice found out that $5P = (4, 0)$.

(a) Using the above information, show that the order of P in the group $(E, +)$ is equal to 10. [*2*]

Hint: determine first the order of the point $(4, 0)$ by working out its inverse in $(E, +)$.

(b) With the help of part (a) and the result of Theorem 2.20 of Chapter 20, determine the order of $(E, +)$ and show that this group is cyclic, without listing any of the remaining elements. [*3*]

(c) Determine the point $P_B = s_B P$. [*2*]

(d) Alice wants to encrypt the message $M = (0, 7) = -P \in E$, choosing a random integer $k = 3$. Determine the points M_1 and M_2 that Alice sends to Bob. [*3*]

(e) Describe Bob's decryption process for Alice's messages M_1 and M_2. [*1*]

Hint: calculations in parts (c) and (d) will simplify if you realise that by parts (a) and (b), every element of $(E, +)$ is a multiple of P.